**AMENDMENTS TO THE CLAIMS:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**LISTING OF CLAIMS:**

1. (Currently Amended) An enciphering method comprising a step of formatting a clear message ~~in clear~~ (m) by means of a formatting function (μ), and a step of exponentiation of the result of the previous step using a public key (N, e) in accordance with the equation $c = \mu(m)^e \bmod N$, c being an enciphered message, μ(m) being the result of the formatting step, and e and N elements of the public key,

~~the method being characterised in that~~ wherein the formatting function (μ) is the PSS function.

2. (Currently Amended) A method according to claim 1, ~~characterised in that~~ wherein the formatting function μ is defined by

$\mu(m) = PSS(m) = \omega \,||\, s$, with:

m, the clear text ~~in clear~~ of k – k0 – k1 bits, r a random parameter of k0 bits, k, k0, k1 being parameters of the formatting function,

|| a concatenation function

$\omega = H(m \,||\, r)$

$s = G(\omega) \oplus (m \,||\, r)$

$\otimes$ a logic function XOR, and

H, G two hashing functions

3. (Currently Amended) ~~Use of~~ A method of enciphering a message using a probabilistic signature function ~~(PSS)~~ defined according to the standard PKCS #2 v 2.1, RSA cryptography standard as a formatting function (μ), ~~in order to effect an enciphering method~~ comprising a step of formatting a clear message ~~in clear~~ (m) by means of the formatting function (μ), and a step of exponentiation of the result of the previous step by means of a public key (N, e) in accordance with the equation $c = \mu(m)^e \bmod N$, c being an enciphered message, μ(m) being the result of the formatting step, and E and N elements of the public key.

4. (Currently Amended) A cryptographic ~~system~~ method comprising:

- a step of formatting a clear message ~~in clear~~ (m) by the probabilistic signature function ~~(PSS)~~, and then:

- if an enciphering of the clear message ~~in clear~~ (m) is required, a step of exponentiation of the result of the formatting step by means of a first key (N, e) in accordance with the equation $c=\mu(m)^e \bmod N$, c being an enciphered message, μ(m) being the result of the formatting step, and e and N elements of the first key, or

- if a signature of the clear message ~~in clear~~ (m) is required, a step of exponentiation of the result of the formatting step by means of a second key (N' d') in accordance with the

equation $s = \mu(m)^{d'} \bmod N'$, s being a signed message, μ(m) being the result of the formatting step, and d' and N' elements of the second key.

5. (Currently Amended) A ~~system~~ method according to claim [[3]] 4, in which the first key and the second key are respectively a public key of a first pair of keys and a private key of a second pair of keys.

6. (Currently Amended) A ~~system~~ method according to claim [[4]] 5, in which the first pair of keys and the second pair of keys are identical.

7. (Currently Amended) A ~~system~~ method according to ~~one of claims 4 to 6,~~ claim 4, in which the enciphering is of the RSA type.

8. (Currently Amended) An electronic component comprising a programmed ~~means~~ processor for implementing an enciphering method according to ~~one of claims 1 to 2~~ claim 1, the programmed ~~means~~ processor comprising ~~in particular~~ a central unit and a program memory.

9. (Currently Amended) An electronic component comprising a programmed ~~means~~ processor for implementing a cryptographic ~~system~~ method according to ~~one of claims 4 to 7~~ claim 4, the programmed ~~means~~ processor comprising ~~in particular~~ a central unit and a program memory.

10. (Currently Amended) A chip card comprising an electronic component according to ~~claim 7 or~~ claim 8.

11. (New) A chip card comprising an electronic component according to claim 9.